

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.



DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : H04L 12/18, H04M 11/02, H04Q 7/08, H04M 17/00, G06F 17/60		A1	(11) Numéro de publication internationale: WO 99/41881 (43) Date de publication internationale: 19 août 1999 (19.08.99)
(21) Numéro de la demande internationale: PCT/FR99/00290		(81) Etats désignés: CA, CN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) Date de dépôt international: 10 février 1999 (10.02.99)		Publiée Avec rapport de recherche internationale.	
(30) Données relatives à la priorité: 98/02295 11 février 1998 (11.02.98) FR			
(71) Déposant (pour tous les Etats désignés sauf US): GEM-PLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).			
(72) Inventeurs; et			
(75) Inventeurs/Déposants (US seulement): CHEVILLON, Laurent [FR/FR]; 121, allée des Goelands, F-34280 La Grande Motte (FR). CANO, Sébastien [FR/BR]; GEMPLUS Do Brasil Ltda, Conjunto 62, Rua Bandeira Paulista #600, CEP-04532-001 São Paulo, SP (BR).			
(74) Mandataire: NONNENMACHER, Bernard; GEMPLUS S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).			

(54) Title: METHOD FOR CONTROLLING THE USE OF A DATA SERVICE TRANSMITTED BY A CENTRAL SERVICE INTENDED FOR PAGING RECEIVERS

(54) Titre: PROCEDE POUR LE CONTROLE DE L'UTILISATION D'UN SERVICE D'INFORMATION EMIS PAR UNE PLATE-FORME CENTRALE A DESTINATION DE MESSAGEURS

(57) Abstract

The invention concerns a method for controlling the use of a data service transmitted by a central platform transmitting for paging receivers operating with credit unit account, said service consisting in transmitting data in the form of messages, characterised in that it comprises the following steps consisting in: encrypting at least part of the data prior to transmission; broadcasting the encrypted data in a message comprising the address of a group of paging receivers; receiving and storing the message on the basis of the user profile contained in the paging receiver and/or a user card (PSIM); decrypting and displaying at least part of the message provided that it is possible to debit by a corresponding amount said credit unit account contained in a card or in the paging receiver.

(57) Abrégé

La présente invention concerne un procédé pour le contrôle de l'utilisation d'un service d'information émis par une plate-forme centrale émettrice à destination de messageurs fonctionnant à l'aide d'un compte d'unité de crédit, ledit service consistant en l'émission d'information sous forme de messages. Il est caractérisé en ce qu'il comporte les étapes suivantes selon lesquelles: on chiffre au moins en partie l'information préalablement à l'émission; on diffuse l'information chiffrée dans un message comportant l'adresse d'un groupe de messageurs; on reçoit et stocke le message en fonction d'un profil d'utilisateur contenu dans le messageur et/ou une carte utilisateur (PSIM); on déchiffre et visualise au moins une partie du message à condition de pouvoir débiter d'un montant correspondant ledit compte d'unités contenu dans une carte ou dans le messageur.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettone	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Liberia	SG	Singapour		
EE	Estonie						

Procédé pour le contrôle de l'utilisation d'un service d'information émis par une plate-forme centrale à destination de messageurs.

La présente invention concerne un procédé pour le contrôle de l'utilisation d'un service d'information émis par une plate-forme centrale émettrice à destination de messageurs fonctionnant à l'aide d'un compte d'unité de crédit, ledit service consistant en l'émission d'information sous forme de messages.

La présente demande a notamment pour objet de préciser et de compléter certains aspects de la demande de brevet FR 96 13370 déposée le 5 juillet 1997 sur l'utilisation d'une carte à puce pour le contrôle d'un système de radio messagerie. Elle est incluse par référence.

Parmi les procédés de ce type, on connaît un procédé qui utilise plusieurs adresses dédiées à des services particuliers. Selon ce procédé, lorsqu'un opérateur vend, sous la forme d'un abonnement mensuel, des services d'information, il peut diffuser chaque type d'information à une adresse donnée. Par conséquent, il y a l'adresse dédiée par exemple aux cours de la bourse, l'adresse dédiée à la météo.

Lorsqu'un utilisateur acquiert un messageur, il s'abonne à un certain nombre des services offerts par l'opérateur. L'opérateur lui remet un messageur contenant une adresse privée, et les adresses des services souscrits.

Ceci impose à un opérateur, lorsqu'un utilisateur désire modifier la liste des services auxquels il est abonné, une lourde et coûteuse reconfiguration de son récepteur (renvoyé au point de vente, voire à l'usine). En outre, ce système ne protège pas l'opérateur dans le cas d'un utilisateur cessant de régler son abonnement (Aucun moyen d'empêcher l'utilisateur de cesser de recevoir le service).

Actuellement, les opérateurs utilisent différentes techniques pour vendre des services, d'autant plus que les messageurs actuels offrent rarement plus de quatre adresses. Les opérateurs ont notamment recours à l'envoi individuel des services, à l'adresse privée, selon les options d'abonnement souscrites par chaque utilisateur, l'avantage étant la souplesse, et l'inconvénient étant l'utilisation d'une bande passante.

La présente invention a pour objectif de pallier aux inconvénients précités.

La présente invention a également et principalement pour objectif de proposer

un moyen plus souple, plus sûr et plus efficace sur le plan de la vente des services, que tous les moyens connus aujourd'hui.

A cet effet, l'invention a pour objet un procédé caractérisé en ce qu'il comporte les étapes suivantes selon lesquelles:

5 - on chiffre au moins en partie l'information préalablement à l'émission, on diffuse l'information chiffrée dans un message comportant l'adresse d'un groupe de messageurs, on reçoit et stocke le message en fonction d'un profil d'utilisateur contenu dans le messager et/ou une carte utilisateur (PSIM), on déchiffre et visualise au moins une partie du message à condition de pouvoir débiter d'un montant correspondant ledit 10 compte d'unités contenu dans une carte ou dans le messager;

- Selon des variantes de mise en oeuvre, le message peut être reçu dans le messager ou dans la carte PSIM; de préférence, on déchiffre et/ou visualise sous condition d'une action volontaire de consultation d'un service par l'utilisateur ; Selon d'autres variantes de mise en oeuvre le message « acheté » donc déchiffré peut être 15 stocké dans le messager ou la carte PSIM;

- on effectue une reconfiguration du messager et/ ou de la carte d'utilisateur (PSIM), en particulier du profil utilisateur par l'émission de commandes exécutables de reconfiguration par voie radio à partir de ladite plate-forme centrale; le cas échéant, on peut également reconfigurer certains menus d'affichage du messager, 20 notamment ceux permettant de guider l'utilisateur vers les services offerts par l'opérateur;

- pour chaque messager, on utilise au moins deux clés de chiffrement, une clé secrète générique partagée par tous les messageurs pour le chiffrement et déchiffrement des messages et une clé personnelle propre à chaque utilisateur pour 25 chiffrer et déchiffrer des commandes exécutables de reconfiguration et/ou rechargement d'unités;

- on porte à la connaissance de l'utilisateur, en particulier par affichage, une partie non chiffrée du message tandis qu'au moins l'autre partie chiffrée est stockée; alternativement, on peut stocker le message entier (partie chiffrée et partie en clair), la 30 partie en clair pouvant être délivrée automatiquement ou sur action volontaire de

l'utilisateur après avertissement, par exemple sonore;

- le message comporte une entête comprenant son prix et sa catégorie pour classifier le message et son prix à l'aide d'une table de services d'information (SAV) disponible en permanence dans le messageur ou dans la carte PSIM;

5 - la plate-forme est apte à générer de nouvelles clés secrètes génériques et/ou clés personnelles et à les transmettre de façon sécurisée par voie radio pour être chargées dans un module de sécurité (PSAM) de chaque messageur et/ou carte d'utilisateur;

10 - chaque profil utilisateur est stocké dans la plate-forme centrale ainsi que dans le module de sécurité du messageur et/ou carte d'utilisateur (PSIM);

- les messages chiffrés sont d'abord stockés dans une mémoire du messageur, puis sur demande de l'utilisateur transféré au PSIM pour déchiffrement, puis délivrés déchiffrés à l'utilisateur, ledit compte étant débité avant le déchiffrement par le PSIM; le déchiffrement du message ne s'effectue pas nécessairement dans la PSIM; cette dernière peut simplement transmettre au messageur la clé « temporaire » permettant de déchiffrer un message donné et unique.

15 - le rechargeement d'unités est effectué sur demande périodique de l'utilisateur auprès d'un centre de service et sur communication d'un identifiant;

20 - ledit centre de service tient à jour un indice/ table de consommation périodique par messageur et/ou par utilisateur;

- on commande l'arrêt ou le fonctionnement du messageur en cas de demande de recharge ment insuffisant par unité de temps établi par chaque indice.

Description.

25 La description qui va suivre apporte des précisions et compléments à la demande de brevet FR 96 13370. Le module de sécurité applicatif décrit ci-après pourra être compris dans le messageur ou dans la carte. Il aura les caractéristiques détaillées dans le brevet en question.

Modification 1:

Le réseau d'émission des messages radio pourra être connecté à une plate-forme de formatage des messages à envoyer. Cette plate-forme pourra également émettre des commandes interprétables par le microprocesseur du messageur.

5 Cette plate-forme a les fonctions ci-après.

Conformément à l'invention, elle a pour fonction de chiffrer certains messages avant qu'ils ne soient transmis par voie radio. (Le chiffrement avant émission des messages est prévu dans la demande de brevet précitée mais on ne parle pas de la plate-forme). Les messages chiffrés pourront être des messages numériques ou 10 alphanumériques privés, adressés à un unique destinataire, ou bien pourront être des informations payantes d'intérêt général (comme des informations sur la météorologie, le trafic, la bourse, etc). Les messages chiffrés par cette plate-forme pourront être diffusés vers une adresse spécifique (vers un destinataire unique identifié par son 15 adresse, ou « Capcode ») ou bien vers une adresse générique, afin d'être reçus par tous les messageurs calés sur la fréquence de l'opérateur émetteur du message (système « broadcast »).

Elle peut encore avoir pour fonction d'assurer le suivi et la gestion des clés 20 secrètes qui serviront à chiffrer les messages avant leur émission et à les déchiffrer à leur réception par le messageur. Au niveau du messageur, ces clés secrètes seront stockées dans le module de sécurité applicatif. Il pourra exister deux classes de clés 25 secrètes : des clés secrètes uniques, propres à chaque module de sécurité, et une clé secrète générique, unique et commune à tous les modules de sécurité contenus dans tous les messageurs d'un opérateur donné. La plate-forme pourra éventuellement générer de nouvelles clés secrètes qui seront envoyées de façon sécurisée par voie radio pour être chargées dans le module de sécurité.

Elle peut encore avoir pour fonction d'assurer le suivi du profil de chaque 30 utilisateur. Chaque utilisateur pourra sélectionner auprès de son opérateur une liste de services auxquels il souhaite avoir accès. Cette information constituera le profil de l'abonné, et ce profil pourra conditionner l'accès à certaines informations payantes (l'abonné pourra ainsi décider de ne pas recevoir dans son messageur d'informations

concernant un ou plusieurs sujet(s) donné(s)). Le profil de chaque abonné sera archivé dans la plate-forme de formatage des messages au niveau du réseau ainsi que dans une zone de mémoire du module de sécurité applicatif. Le module de sécurité applicatif réalise le filtrage des messages de service en fonction du profil-utilisateur qu'il 5 contient. Ce profil contenu dans le module de sécurité applicatif pourra être modifié à distance par opérateur grâce à des commandes exécutables par voie radio depuis la plate-forme de formatage.

Elle peut encore avoir pour fonction d'assurer le rechargeement sécurisé à 10 distance (par voie radio) d'un compteur contenu dans une zone de mémoire du module de sécurité utilisé dans le messageur. Le compteur pourra être recharge à distance par l'envoi de messages exécutables émis depuis la plate-forme de formatage.

Elle peut également avoir la fonction d'assurer le suivi et la mise à jour des 15 menus applicatifs affichés à l'écran du messageur et stockés dans une zone de mémoire du module de sécurité. Différents menus et options pourront être affichés à l'écran du messageur (voir modification numéro 2 ci-dessous). Ces menus pourront être contrôlés et modifiés depuis la plate-forme de formatage contenue dans le réseau 20 d'émission des messages radio.

Modification 2:

20 Comme indiqué dans la demande de brevet précitée, le messageur pourra contenir un module de sécurité applicatif. Ce module de sécurité applicatif pourra remplir les fonctions suivantes énumérées ci-après dans l'utilisation du messageur.

Il peut contenir, dans sa zone de mémoire, un compteur rechargeable d'unités 25 financières. La valeur financière contenue dans ce compteur pourra être affichée et consultée à tout moment par l'utilisateur du messageur.

Le rechargeement du compteur peut se faire :

- soit par l'insertion d'une carte à puce (à microprocesseur ou à mémoire) dans 30 le messageur, comme cela est décrit dans le brevet principal. La carte servant à recharger la valeur du compteur contenu dans le module de sécurité pourra être insérée en permanence dans le messageur ou uniquement de façon momentanée, le temps de

transférer une valeur financière donnée de la carte vers le compteur du module de sécurité.

- soit à distance, par voie radio, en envoyant depuis la plate-forme de formatage une commande de recharge du compteur contenu dans le module de sécurité. Cette commande sera chiffrée par la plate-forme de formatage à l'aide d'une des clés secrètes contenues dans la base de données des clés secrètes et sera déchiffrée dans le module de sécurité à l'aide de la même clé, contenue dans sa zone de mémoire.

Le module de sécurité peut contrôler l'accès de messages chiffrés. Les messages envoyés à travers la plate-forme de formatage pourront être chiffrés avant leur émission (comme décrit dans la Modification 1) et stockés soit dans la mémoire du messageur, soit dans la mémoire du module de sécurité. Ces messages pourront être des messages privés ou bien des messages d'information générale (messages d'information dits communément message de Service à Valeur Ajoutée).

Les messages privés peuvent être automatiquement déchiffrés par le module de sécurité (ou par le messageur à l'aide des clés secrètes contenues dans le module de sécurité) puis affichés après que le module de sécurité ait débité la valeur dudit message dans son compteur. Dans ce cas, si le crédit du compteur est inférieur à la valeur du message, le message pourra être stocké sous forme chiffrée dans la mémoire du messageur ou dans la mémoire du module de sécurité, sans avoir été préalablement affiché.

Les messages privés peuvent également déclenchés, dès leur réception dans le messageur, un signal d'avertissement pour l'utilisateur qui aura alors la possibilité de consulter ledit message (et donc de faire déduire son prix de la valeur contenue dans le compteur du module de sécurité) ou bien de le refuser, et de l'effacer de la mémoire du messageur (ou du module de sécurité) sans avoir été consulté. Dans ce dernier cas, la valeur du message n'est pas débitée du compteur contenu dans le module de sécurité.

Les messages d'information générale (messages de Service à Valeur Ajoutée) seront stockés dès leur réception sous leur forme chiffrée soit dans la mémoire du messageur, soit directement dans la mémoire du module de sécurité. Certains de ces

messages pourront contenir un ordre d'effacement de messages déjà stockés (par exemple s'il s'agit de l'actualisation d'une rubrique déjà contenue en mémoire). Ces messages d'information pourront contenir une partie de texte non chiffrée et affichable permettant à l'utilisateur de connaître le type d'information contenue (résultat sportif, 5 tirage du loto, etc...).

L'entête du message pourra indiquer le type du message (catégorie) ainsi que son prix de consultation. Lorsque l'utilisateur souhaitera consulter une de ces informations générales contenues dans la mémoire du messageur ou du module de sécurité, il pourra alors (à travers l'interface utilisateur du messageur) donner l'ordre 10 au messageur de déchiffrer son contenu. Le prix du message sera d'abord débité de la valeur du compteur contenu dans le module de sécurité, et le message sera déchiffré soit par le messageur (à l'aide de la clé secrète générique contenue dans le module de sécurité), soit par le module de sécurité lui même. Le message déchiffré pourra être stocké soit dans la mémoire du messageur, soit dans la mémoire du module de sécurité. 15

Le module de sécurité peut contenir le profil de l'utilisateur tel que celui-ci aura été défini au préalable (au moment de la demande d'abonnement par exemple). Le profil de l'utilisateur permettra de filtrer les informations générales reçues et d'éviter un encombrement de la mémoire disponible avec des informations sans intérêt 20 pour l'utilisateur. Ainsi, si l'utilisateur n'est pas intéressé par un type d'information donné, par exemple : les informations financières, tous les messages d'information générale diffusés sous cet intitulé (qui apparaît dans l'en-tête du message, comme décrit dans le point précédent) ne seront pas stockés en mémoire. Comme vu dans la Modification 1, le profil d'utilisateur pourra être modifié à distance par l'envoi de 25 commandes à distance dans le module de sécurité depuis la plate-forme de formatage.

Le module de sécurité peut contenir dans sa zone de mémoire, toutes les informations nécessaires à la personnalisation du messageur. En effet, dans le cas où le module de sécurité est prévu sous une forme extractible (par exemple : une carte à puce ou « mini-carte à puce » au format ID-000), le messageur pourra être fabriqué et 30 distribué sous une forme complètement générique. Aucune information spécifique ne

sera contenue dans sa mémoire (aucun numéro de série, adresse de fréquence, « capcode » ne seront nécessaires). Les informations permettant de lier ce messageur à un opérateur particulier (adresse de la fréquence d'opération, « capcodes ») seront intégralement contenues dans le module de sécurité. Le messageur deviendra un produit totalement anonyme qui pourra être distribué directement par le fabricant, sans avoir à passer par une étape de programmation de la mémoire (destinée à faire fonctionner le messageur sur un réseau donné, pour un opérateur donné). L'utilisateur, qui aura obtenu de son opérateur un module de sécurité extractible lors de son abonnement (par exemple, une carte à puce ou « mini-carte à puce »), n'aura plus qu'à insérer le module en question dans le messageur générique pour rendre ce dernier opératoire sur le réseau de son opérateur.

Le module de sécurité peut également contenir le détail des menus accessibles depuis l'interface utilisateur du messageur. Ces menus pourront être modifiés à distance par l'envoi par voie radio de commandes exécutables dans le module de sécurité.

L'invention a également pour objet de proposer un procédé permettant de savoir si l'utilisateur utilise régulièrement son messageur, et donc s'acquitte financièrement du service. Comme il est probable que le messageur soit donné gratuitement ou à un prix réduit, il est souhaitable en cas de non utilisation, de pouvoir le récupérer ou du moins interdire un quelconque usage. Ceci est nécessaire du fait du principe de fonctionnement unidirectionnel des messageurs.

Selon d'autres caractéristiques, on peut inciter l'utilisateur à effectuer un rechargement d'unités périodiquement auprès d'un centre de service par exemple sur communication d'un identifiant. A cet effet, on peut envoyer un message d'avertissement demandant à l'utilisateur de recharger ou de faire une action quelconque. Alternativement, sans avertissement, l'utilisateur sait qu'il doit recharger une somme minimale périodiquement.

Pour réaliser cette fonction, il est prévu que le centre de service comporte des moyens informatiques pour tenir à jour un indice ou une table de consommation périodique par messageur et/ou utilisateur.

Ces moyens informatiques ont la capacité de commander l'arrêt ou le fonctionnement du messageur en cas de demande de rechargement insuffisant par unité de temps établi par chaque indice ou pour toute autre raison. Ces moyens informatiques ont également la capacité d'empêcher momentanément l'usage du messageur pendant une phase de rechargement ou de reconfiguration.

REVENDICATIONS

1. Procédé pour le contrôle de l'utilisation d'un service d'information émis par une plate-forme centrale émettrice à destination de messageurs fonctionnant à l'aide d'un compte d'unité de crédit, ledit service consistant en l'émission d'information sous forme de messages, caractérisé en ce qu'il comporte les étapes suivantes selon lesquelles:
 - on chiffre au moins en partie l'information préalablement à l'émission,
 - on diffuse l'information chiffrée dans un message comportant l'adresse d'un groupe de messageurs,
 - 10 - on reçoit et stocke le message en fonction d'un profil d'utilisateur contenu dans le messageur et/ou une carte utilisateur (PSIM)
 - on déchiffre et visualise au moins une partie du message à condition de pouvoir débiter d'un montant correspondant ledit compte d'unités contenu dans une carte ou dans le messageur.
- 15 2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend une étape selon laquelle on effectue une reconfiguration du messageur et/ ou de la carte d'utilisateur (PSIM), en particulier du profil utilisateur par l'émission de commandes exécutables de reconfiguration par voie radio à partir de ladite plate-forme centrale.
- 20 3. Procédé selon l'une des revendications précédentes, caractérisé en ce que pour chaque messageur, on utilise au moins deux clés de chiffrement, une clé secrète générique partagée par tous les messageurs pour le chiffrement et déchiffrement des messages, et une clé personnelle propre à chaque utilisateur pour chiffrer et déchiffrer des commandes exécutables de reconfiguration et/ou rechargement d'unités.
- 25 4. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'on porte à la connaissance de l'utilisateur, en particulier par affichage, une partie non chiffrée du message tandis que l'autre partie chiffrée est stockée.
- 30 5. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message comporte une entête comprenant son prix et sa catégorie pour classifier le message et son prix à l'aide d'une table de services d'information (SAV) disponible en permanence dans le messageur.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que la plate-forme est apte à générer de nouvelles clés secrètes génériques et/ou clé personnelle et à les transmettre de façon sécurisée par voie radio pour être chargées dans un module de sécurité (PSAM) de chaque message et/ou carte d'utilisateur.

5 7. Procédé selon l'une des revendications précédentes, caractérisé en ce que chaque profil utilisateur est stocké dans la plate-forme centrale ainsi que dans le module de sécurité du messageur et/ou carte d'utilisateur (PSIM).

10 8. Procédé selon l'une des revendications précédentes, caractérisé en ce que les messages chiffrés sont d'abord stockés dans une mémoire du messageur, puis sur demande de l'utilisateur transféré au PSIM pour déchiffrement, puis délivrés déchiffrés à l'utilisateur, ledit compte étant débité avant le déchiffrement par le PSIM.

9. Procédé selon l'une des revendications précédentes, caractérisé en ce que le rechargement d'unités est effectué sur demande périodique de l'utilisateur auprès d'un centre de service et sur communication d'un identifiant.

15 10. Procédé selon l'une des revendications précédentes, caractérisé en ce que le centre de service tient à jour un indice/table de consommation périodique par messageur et/ou par utilisateur.

20 11. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'on commande l'arrêt ou le fonctionnement du messageur en cas de demande de rechargement insuffisant par unité de temps établi par chaque indice.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00290

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04L12/18 H04M11/02 H04Q7/08 H04M17/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 IPC 6 H04L H04M H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 90 02382 A (INDATA CORP) 8 March 1990 see abstract see page 2, line 16 - page 3, line 8 see page 5, line 9 - page 9, line 29 see page 17, line 19 - page 18, line 23 see page 25, line 10 - page 26, line 7 see page 29, line 4-9 see page 39, line 21-25 ---	1,2 3-5,8-11
Y	EP 0 538 933 A (PHILIPS ELECTRONICS UK LTD ;PHILIPS NV (NL)) 28 April 1993 see abstract see column 1, line 26 - column 5, line 30 see figure 1 ---	1,2
A	US 5 283 832 A (LOCKHART JR ROBERT K ET AL) 1 February 1994 see column 1, line 18-24 ---	1,2 -/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

6 May 1999

Date of mailing of the international search report

17/05/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl
Fax: (+31-70) 340-3016

Authorized officer

Lievens, K

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00290

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 285 496 A (FRANK EDWARD H ET AL) 8 February 1994 see abstract see column 3, line 52 - column 4, line 40	3

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No

PCT/FR 99/00290

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9002382	A 08-03-1990	AT 166986	T	15-06-1998
		AU 4188289	A	23-03-1990
		DE 68928694	D	09-07-1998
		DE 68928694	T	17-12-1998
		EP 0472521	A	04-03-1992
		US 5247575	A	21-09-1993
EP 0538933	A 28-04-1993	DE 69219991	D	03-07-1997
		DE 69219991	T	27-11-1997
		JP 5218946	A	27-08-1993
		SG 48347	A	17-04-1998
		US 5371493	A	06-12-1994
US 5283832	A 01-02-1994	NONE		
US 5285496	A 08-02-1994	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Demai internationale No

PCT/FR 99/00290

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
 CIB 6 H04L12/18 H04M11/02 H04Q7/08 H04M17/00 G06F17/60

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
 CIB 6 H04L H04M H04Q G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y A	WO 90 02382 A (INDATA CORP) 8 mars 1990 voir abrégé voir page 2, ligne 16 - page 3, ligne 8 voir page 5, ligne 9 - page 9, ligne 29 voir page 17, ligne 19 - page 18, ligne 23 voir page 25, ligne 10 - page 26, ligne 7 voir page 29, ligne 4-9 voir page 39, ligne 21-25 ---	1,2 3-5,8-11
Y	EP 0 538 933 A (PHILIPS ELECTRONICS UK LTD ;PHILIPS NV (NL)) 28 avril 1993 voir abrégé voir colonne 1, ligne 26 - colonne 5, ligne 30 voir figure 1 ---	1,2 -/-

Voir la suite du cadre C pour la fin de la liste des documents

Les documents de familles de brevets sont indiqués en annexe

Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

6 mai 1999

Date d'expédition du présent rapport de recherche internationale

17/05/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
 Office Européen des Brevets, P.B. 5018 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
 Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Lievens, K

RAPPORT DE RECHERCHE INTERNATIONALE

Demar. Internationale No
PCT/FR 99/00290

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 283 832 A (LOCKHART JR ROBERT K ET AL) 1 février 1994 voir colonne 1, ligne 18-24 ---	1,2
A	US 5 285 496 A (FRANK EDWARD H ET AL) 8 février 1994 voir abrégé voir colonne 3, ligne 52 - colonne 4, ligne 40 ---	3

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demar. Internationale No

PCT/FR 99/00290

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9002382 A	08-03-1990	AT 166986 T AU 4188289 A DE 68928694 D DE 68928694 T EP 0472521 A US 5247575 A	15-06-1998 23-03-1990 09-07-1998 17-12-1998 04-03-1992 21-09-1993
EP 0538933 A	28-04-1993	DE 69219991 D DE 69219991 T JP 5218946 A SG 48347 A US 5371493 A	03-07-1997 27-11-1997 27-08-1993 17-04-1998 06-12-1994
US 5283832 A	01-02-1994	AUCUN	
US 5285496 A	08-02-1994	AUCUN	